量子アニーリングマシンを用いた素因数分解

修士学位論文要約（平成31年３月）

量子アニーリングマシンを用いた素因数分解

三上　譲治
指導教員：田中　和之，　学位論文指導教員：大関　真之

Prime Factorization using quantum annealing machines

Joji MIKAMI
Supervisor: Kazuyuki TANAKA,　Research Advisor: Masayuki Ohzeki

Prime factorization has been used for a secure data transmission because it is widely believed to be NP-complete. We construct the way of converting the prime factorization problem into the ising model for using the quantum annealing machine. However, it is difficult to get the optimal solution in big problems by the present quantum annealing machine. To increase the probability that the optimal solution appears, we propose the method of reducing the size of the problem and searching the exact solution around the approximate one that is mostly appeared in trials. We have performed experiments of the performance on our method and the reverse annealing that is physically done for the local search. Compared to the reverse annealing, our proposed algorithm can frequently get the optimal solution around the approximate one.

1. はじめに

素因数分解とは，ある正の整数Mに対して$M = ab$を満たす 2 つの素数a, bを見つける問題である．素数の桁数が大きい場合では計算困難であるので，インターネット通信の安全性を確保するための暗号化に利用されている．この計算困難な問題を対処する方法の一つとして，量子アニーリング [1]の理論に沿って作られた装置である量子アニーリングマシンを利用しようとする試みが近年注目されている．量子アニーリングマシンが，カナダのベンチャー企業 D-Wave System によって開発された．量子アニーリングは，最適化問題の厳密解を量子力学的な揺らぎを加えて探索する手法である．量子ビットへの局所磁場や相互作用を指定し，量子ビットのチップを極低温に冷却すると，量子ビット全体が自然にエネルギーの最も低い状態（基底状態）になろうとする．最小化したい関数をマシンに利用できるイジング模型の形式で表現することができれば，その関数を最小化する変数を物理的に求めることができると言える．

量子アニーリングマシンであるD-Wave マシンには利用できる数理的モデルに対し様々な制約がある．第一に，量子ビット同士に相互作用をもたらす結合が全結合ではなく疎ということである．第二に，相互作用ができる量子ビットは2体までしかないということである．3体以上の相互作用を2体相互作用にする方法は存在するが，そのためには新しい変数を用意しなければならなくなる．量子ビットの数が増加するにつれて厳密解が出現する確率は低下していき，エネルギーの低い近似解ばかり出現するようになる．本研究では，量子アニーリングマシンを用いて素因数分解をするコスト関数を設計し，厳密解を出現する割合を上昇させるために使用する変数を削減する方法と，多数出現する近似解を利用する手法を検討した．

2. 素因数分解のイジング模型表現

2体相互作用と局所磁場のあるイジング模型のハミルトニアン$H(\boldsymbol{\sigma})$の基底状態を求める問題は組合せ最適化である．あるJ_{ij}, h_iが与えられたときに，$H(\boldsymbol{\sigma})$を最小とする$\boldsymbol{\sigma}$を求めよ，という最適化問題を量子アニーリングマシンで解くことができる．ある整数Mは素数a, bの積であるとする．2進数で表現されたa, bを筆算した計算結果がMになるときにエネルギーが0になるようにコスト関数を設計した．そのコスト関数を最小化する解を量子アニーリングマシンで取り出したとき，Mを素因数分解したa, bを得ることができる．

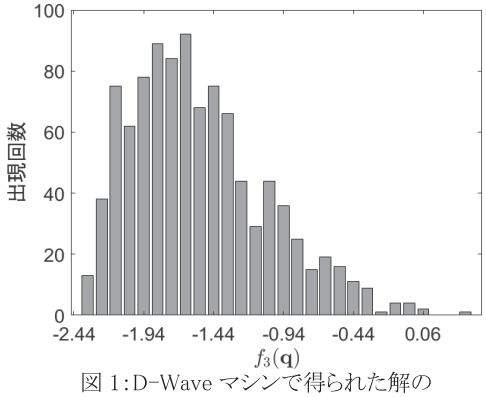

図 1：D-Wave マシンで得られた解のエネルギー$f_3(\boldsymbol{q})$と出現回数

3. 量子アニーリングマシンによる実験

実際に量子アニーリングマシン D-Wave マシンで $23 \times 29 = 667$を素因数分解するコスト関数を設計し，これを$f_3(\boldsymbol{q})$とした．試行回数 1000 回で$f_3(\boldsymbol{q})$を D-Wave マシンに送信して得られた解のエネルギーと出現回数の分布を図 1 に示す．厳密解は 1000 回中 1 回しか出現せず，図 1 を見ても厳密解よりエネルギーの高い解ばかり頻出したことが分かった．この実験を通して，現行の D-Wave マシンは使用する変数がある程度多い問題では厳密解を返すのが難しいということが分かった．

4. 使用変数の削減と解の再利用

組合せ最適化問題では変数が多くなると解空間が指数関数的に広がるので，厳密解を得られる確率は低下する．これを防ぐ簡単な方法はまず使用する変数を削減することである．コスト関数を構成する制約式から，ある変数を別の変数の従属変数にしたり，実現値を確定するなどして使用変数を削減した．

しかし，変数を削減することにも限界があるので，変数が多いままだとやはり厳密解ではなく近似解ばかり出現する問題は残されている．ところが，その近似解は厳密解とハミング距離が近い解となる傾向がある．そこで本研究では多数出現する近似解を再利用する方法として，指定した近似解から局所探索する手法を提案した．局所探索したいスピングラスのハミルトニアンを$H(\boldsymbol{\sigma})$とし，得られたエネルギーの低い近似解を$\boldsymbol{\sigma}'$とする．$\boldsymbol{\sigma} = \boldsymbol{d} \odot \boldsymbol{\sigma}'$を満たす新しいイジング変数$\boldsymbol{d}$を用意し，$H(\boldsymbol{d})$に書き直す．その後，新しい$H(\boldsymbol{d})$のすべての相互作用に対し任意の負の$\rho$を加える．これを式(1)に示す．

$$H(\boldsymbol{d}) = -\sum_{i<j} \left(J_{ij}\sigma_i'\sigma_j' - \rho\right) d_i d_j - \sum_{i=1}^{N} h_i \sigma_i' d_i \quad \ldots (1)$$

大きなρが加わると全てのスピン$\boldsymbol{d}$に強磁性相互作用が働き，dは同じ向き(+1)になろうとするので，$\boldsymbol{\sigma} = \boldsymbol{\sigma}'$となることが基底状態になる．適切な$\rho$を選択すると，$\boldsymbol{\sigma}'$とハミング距離が近い解がエネルギーが低くなるので，$\boldsymbol{\sigma}'$の周辺を探索をすることができる．この提案手法について実験を通して確かめた．$17 \times 31 = 527$を素因数分解するコスト関数を設計し，これを$f_4(\boldsymbol{q})$とした．提案手法の比較として，リバースアニーリング [2]についても実験した．リバースアニーリングは，アニーリング中の横磁場の変化の仕方を変え，指定した初期状態からアニーリングを開始する手法であり，局所探索をする手法である．初期状態をどの程度重要視するかを決めるパラメータを変化させて，試行回数 1000 回で初期状態と厳密解が何回出現したかを図 2 に示す．図 2 から，リバースアニーリングに比べて提案手法は厳密解を出現させる割合が増加したことが分かった．その後，初期状態を変化させたときに提案手法がどの程度有効に働くかを調べた実験を行ったが，ここでは省略する．

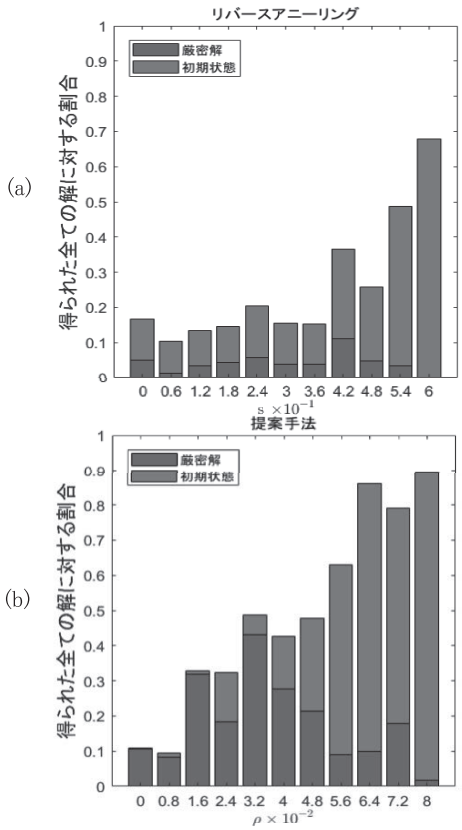

図 2:リバースアニーリング(a)と提案手法(b)における局所探索の性能比較

5. まとめ

本論文では，実際に稼働している量子アニーリングマシンを用いて，組合せ最適化問題である素因数分解を実行する方法を構築した．また，規模が大きくなるにつれて厳密解が出現しにくくなるという課題があるので，厳密解を出現させる確率を高めるために，制約式から使用する変数を削減することで問題の規模を縮小させる方法と，エネルギーが低い近似解を再利用してその近傍を探索して厳密解を見つけ出しやすくする提案手法について述べた．提案手法は QUBO 行列の構造に依存せずに適用できるので，素因数分解に限らず様々な最適化問題を量子アニーリングマシンを通して解く場合において局所探索をしてエネルギーの低い解を発見できる可能性があると分かった．

文献

1) T Kadowaki, and H Nishimori. Physical Review E 58.5 (1998): 5355.
2) Perdomo-Ortiz, Alejandro, Salvador E. Venegas-Andraca, and Alán Aspuru-Guzik. Quantum Information Processing 10.1 (2011): 33-52.